Preparing Governments for Future Shocks

Building Cyber Resilience Roundtable:

Read Ahead Materials

Introduction to the Future Shocks Initiative

Government leaders increasingly indicate that what were previously viewed as Black Swan events are now becoming more frequent — and more destabilizing — shocks. The past three years saw acceleration toward a connected world where physical goods and digital services are increasingly interdependent. The vulnerability of social and economic well-being is laid bare by reliance on connectivity and distributed value chains subject to disruption on multiple fronts.

Risks have grown due to complex variables such as geopolitical conflicts, multiple public health emergencies, climate-related natural disasters (wildfires, hurricanes, drought), the breakdown of longstanding trade relationships, economic displacement, and economic inequality. The combination of these factors renders current planning models obsolete.

Citizens, non-governmental organizations, and commercial enterprises continue to rely on governments to help manage these uncertainties. However, traditional incident response frameworks may no longer be sufficient, as events occur across multiple domains, jurisdictions, and decision-making authorities. Rather, collaborative action to address anticipated threats requires focus and cooperation across a broad ecosystem of partners and stakeholders. Governments must prepare for "future shocks" by supporting stakeholders with insights, resources, innovation, and adaptation that characterizes a successful response to any high-impact event.

IBM, working through the IBM Center for The Business of Government and the IBM Institute for Business Value, and in partnership with the National Academy of Public Administration (NAPA), has launched an initiative to help government identify core capabilities critical to building such resilience, and make progress toward addressing major national and international priorities including the Grand Challenges in Public Administration put forth by NAPA.

Through this initiative, we are convening a series of international roundtable discussions with global leaders from across the public, private, academic, and non-profit sectors to capture lessons across six key domain areas: Emergency Preparedness and Response, Cybersecurity, Supply Chain, Sustainability, Workforce Skills, and International Cooperation. In each domain, we will harvest insights from the roundtables to identify strategies and solutions for governments to act. The first roundtable convened leaders in emergency management for an insightful discussion of actionable, and practical steps to build resilience by preparing for future shocks. Learn more about the initiative by reading the blog, 'Preparing Governments for Future Shocks' or listening to the podcast interview with Michael J Keegan, IBM Center for The Business of Government.

Cyber Resilience – Highlights from Research

In the realm of cybersecurity, tremendous knowledge and experience have grown at all levels of government around responding to high-impact events, such as SolarWinds, recent Microsoft Exchange Server exploits, the OPM data breach, and the Colonial Pipeline ransomware attack.

A vast body of research literature informs the topics of cyber risk and cyber resilience. Yet for cybersecurity incident response, the most helpful knowledge is often empirical. Practical insights are complex and nuanced, with essential contributions from diverse stakeholders including the general public, business community, civil society, academia, and all levels of government.

To focus the roundtable discussion on actionable insights, below are key themes that point to actions for building cybersecurity resilience. The topics focus on each of the two discussion items in the agenda, and the questions following each topic will form the basis for discussion (refined based on top three priorities as identified by participants). Exploring these topics in depth through the Roundtable will help prepare governments to address future cyber shocks.

Protecting Critical Infrastructure

1. **Fostering resilience and continuity of operations** – threats to undermine both organizational resilience and continuity of operations include shocks such as ransomware, and climate catastrophe.
    a. How can governments define a base level of preparedness required to withstand shocks and continue to provide essential citizen services?
2. **Adapting governance to a shared responsibility model** – governments must plan for and evaluate cybersecurity governance in terms of defining responsibility for defense and resilience, and develop policies and standards that align to agency missions (including modernizing security governance to support the implementation of zero trust principles).
    a. How can partners best work across the broader ecosystem in addressing potential threats and the societal impact of cyber-attacks?
3. **Coordinating with stakeholders across all levels of government** – threats exist at all levels of government - namely national, state, local, tribal, and territorial. Some actions to take involve combining resources, activating public-private partnerships, coordinating incident response, and sharing leading practices.
    a. How can communication informed by cyber expertise help governments understand policy gaps, implement coordinated policy solutions, and still maintain privacy?
4. **Modernizing security of critical infrastructure** – defending critical infrastructure requires both an understanding of systems and a defense strategy that repels attacks but also has robust intrusion response.
    a. How can governments work with industry to help make security intrinsic to infrastructure architecture and system design and more friction-less for end users?

5. **Standardizing cyber incident response** – an incident response strategy must be established well before a cyber incident. This should include robust testing and training processes and an efficient communications framework.
    a. How can governments identify and engage stakeholders across domains?

Enabling Hybrid and Distributed Work

6. **Using automation and connectivity to optimize capacity, skills, and resources**– building new capabilities around connected devices and connected services, embracing modernization and emerging technologies, and developing new technologies that keep pace with advancing threats.
    a. How can governments work with industry and academia to stay ahead of the innovation curve and develop resilient systems given potential threats to cyber, physical, and natural hazards?
7. **Improving security hygiene** – understanding the collective impact of human behavior. Developing strong cyber hygiene for all individuals acting in both private and professional capacities is essential.
    a. What strategies can all stakeholders take to promote security "ABCs "-- awareness, behaviors, and culture?
8. **Developing the cyber workforce** – anticipating skill demand, identifying talent gaps, and attracting and retaining talent in key security positions represents an issue that for government and industry are dealing with in many domains – issues addressed in a recent congressionally mandated NAPA report for DHS CISA.
    a. How can we meet current and future cybersecurity demand, via better engagement with traditional and non-traditional sources of talent?
9. **Re-envisioning technology, security, and data integrity as public goods –** security concerns exist for many forms of technology that are based on implicit trust, including the dissemination of misinformation and disinformation through social media. Additionally, many platforms operate across multiple levels of government and across international borders, introducing complex operational and compliance demands.
    a. How can leaders reinforce the public's ability to securely access networks with accurate, high-value information anytime, anyplace, anywhere?
10. **Recognizing the significance of emerging technologies, including quantum computing** – anticipating new threats from technology innovations, including the dangers posed to existing digital encryption protocols by quantum exploits as well as new ways of working with solutions based on distributed (vs centralized) authority (e.g. consensus-based solutions, distributed ledgers)
    a. How should governments prepare for the future by addressing security vulnerabilities created by new technologies such as quantum computing and blockchain?

Key Reports for Reference

The World Economic Forum report The Global Risks Report 2022, 17th Edition Insight Report discusses how the COVID-19 pandemic has affected the world and the tension that will arise from governments recovering and responding to different threats – including cyber vulnerabilities.

The International Monetary Fund (IMF) report, The Global Cyber Threat, provides insight into the present and future cyber risks that plague global financial systems. And, despite this constant threat to financial stability, the question remains on who the responsible party is for protecting the system.

The Cybersecurity & Infrastructure Security Agency (CISA) Strategic Plan (2023 – 2025) report discusses the plan developed around how the nation will collectively reduce risk and build resilience to cyber and physical threats to the nation's infrastructure, describing four goals to drive change over four key areas. CISA also published the report A Guide to Critical Infrastructure Security and Resilience detailing the approach to critical infrastructure security and resilience adopted in the U.S. to enhance domestic and global security. Additionally, The White House Executive Order on Improving the Nation's Cybersecurity focuses on updated federal guidance that federal agencies will implement going forward.

The OECD report, Recommendation of the Council on Digital Security of Critical Activities, provides guidance to governments on strengthening the digital security of operators of such critical activities without imposing unnecessary burdens on other actors.

IBM's Institute for Business Value, working with the IBM Center for The Business of Government, issued the report Government transformation in tumultuous times. This report examines how in response to massive disruption, government leaders have to act quickly and decisively to show citizens they're capable of navigating crisis and change.

In addressing the 12 Grand Challenges in Public Administration, the National Academy of Public Administration published a spotlight report on Managing Technological Changes. This report provides insight into the opportunity for the government to better serve its citizens and solve problems more quickly and effectively while firstly ensuring that they address the risks to citizens' economic, security, and private interests.

The National Academy of Public Administration also recently published A Call to Action: The Federal Government's Role in Building a Cybersecurity Workforce for the Future. This congressionally mandated study for CISA examined the government-wide cybersecurity workforce development strategy and CISA's strategy for developing the nation's cybersecurity workforce and its partnership models. The report found that CISA and other agencies have made progress on individual cybersecurity workforce development programs; however, the absence of a government-wide cybersecurity workforce development strategy and lack of clarity about federal agency roles and responsibilities has hindered the federal government's ability to tap the capabilities and resources in the private sector, academia, and other levels of government. The report offers recommendations related to this government-wide strategy and the governance structure required.

The Cyberspace Solarium Commission report 2022 Annual Report on Implementation examines the significant improvements in U.S. cybersecurity, citing critical legislation, increased funding for government cybersecurity efforts, and cybersecurity strategy and policy implementation across the government. However, this implementation is not equal to success – consistent improvements are required to reach national cyber resilience and the agility to address the ever-shifting threat landscape.

The Aspen Institute report Principles for Growing and Sustaining the Nation's Cybersecurity Workforce discusses the cybersecurity skills gap and the major trends contributing to the gap and ultimately, provides eight recommendations for consideration to close the cybersecurity skills gap. IBM's Federal Ecosystem Executive Order Implementation initiative, has convened a working group with the goal to help accelerate federal agency's progress against the current administration's Executive Order on Improving the Nation's Cybersecurity (referenced above). For most organizations, a zero-trust approach represents not just a fundamental shift in how they approach cybersecurity, but an array of acronyms, pitches, and slogans that can potentially confuse and distract from the objective: mitigating the risk of cyber-attacks. The initial project as a working group is to review and identify best practices and gaps in existing zero trust frameworks and assets, paying special attention to segments where the IBM Ecosystem collaborative approach can make the most impact – common lexicon, maturity model, skills, software code, application of the MITRE's ATT&CK framework and implementation roadmap. The first deliverable – included here– defines a zero-trust lexicon. All are invited to review, improve, and use.

The ISTARI report, Cyber Crisis Preparedness: How to Craft a Winning Playbook, shares an interview with Jo De Vliegher, former CIO at Norsk Hydro and now a client partner at ISTARI, and discusses his experience and what he has learned about preparedness and resilience when it comes to cybersecurity.